REMARKS

Claims 1 – 38 were pending in this application when last examined. In the office action dated September 13, 2001, the Examiner rejected claims 1, 15, 29, 30, 31, 37, and 38 and objected to all other claims (as indicated to the applicant's representative in a voicemail received on March 6, 2002).

In response, applicant is canceling claim 1, amending claim 6, which was objected to, to include the limitations of base claim 1, and amending claims 2 –5 and 7 – 14 so that they depend from claim 6. Accordingly, claims 2 – 14 are now believed to be allowable.

With respect to claims 15 – 28, applicant is canceling claim 15, amending claim 20, which was objected to, to incorporate the limitations of base claim 15, and amending claims 16 – 19 and 21 – 28 to depend from claim 20. Accordingly, applicant respectfully submits that claims 16 – 28 are now allowable.

With respect to claims 29 and 30, applicant is amending claims 29 and 30 to include a limitation substantially similar to the limitation in claim 6, which was indicated as objectionable. Accordingly, applicant submits that claims 29 and 30 are now allowable.

With respect to claims 31 – 36, applicant is canceling claim 31, incorporating the limitations of claim 31 into claim 32, which was objected to, and amending claims 33 – 36 to depend from claim 32. Accordingly, applicant submits that claims 23 – 36 are now allowable.

With respect to claims 37 and 38, applicant is amending claims 37 and 38 to include limitations substantially similar to claim 32 and therefore, applicants submit that claims 37 and 38 should also be allowable for at least the same reasons.

Applicants believe that this application is now in condition for allowance of claims 2 –14, 16 – 30, 32 – 38, as amended, and, therefore, an early Notice of Allowance is respectfully requested.

If the undersigned attorney has overlooked a teaching in any of the cited references that is relevant to the allowability of the claims, the Examiner is respectfully requested to specifically point out where such teaching may be found.

Attached hereto is a marked-up version of the changes made to the specification and claims by the current amendment. The attached page is captioned "**VERSION WITH MARKINGS TO SHOW CHANGES MADE.**"

If the Examiner has any questions or needs any additional information, the Examiner is invited to telephone the undersigned attorney at (650) 843-3375. If for any reason an insufficient fee has been paid, please charge the insufficiency to Deposit Account No. 05-0150.

Date: 3/7/02

Squire, Sanders & Dempsey L.L.P.
600 Hansen Way
Palo Alto, CA 94304-1043
Telephone (650) 856-6500
Facsimile (650) 856-3619

Respectfully submitted,

Aaron Wininger
Attorney for Applicant
Registration No. 45,229

VERSION WITH MARKINGS TO SHOW CHANGES MADE

In the Claims:

Delete claim 1.

2. (Twice amended) The system of claim [1] 6, wherein the communications engine uses SSL to create a secure communications link with the client.

3. (Once Amended) The system of claim [1] 6, wherein the communications engine negotiates an encryption protocol for transferring messages to and from the client.

4. (Once Amended) The system of claim [1] 6, wherein the communications engine uses public key certificates for transferring messages to and from the client.

5. (Thrice amended) The system of claim [1] 6, wherein the security services use public key certificates to authenticate a user of the client to determine the client privileges.

6. (Thrice amended) [The system of claim 1, wherein] A system on a server computer system, comprising:

a communications engine for establishing a communications link with a client;

security services coupled to the communications engine for determining client privileges, the security services further capable to examine the identity of a user of the client and the level of authentication to determine the client privileges;

a web server for enabling the client to select a service from a set of available services, the set of available services based on the client privileges;

a host engine coupled to the security services and to the web server for providing to the client service communication code that enables communication with a selected service; and

a keysafe for storing keys, each key for enabling communication between the client and a respective service from the set of available services, thereby enabling the

client to access the available services without storing the service communication code and keys at the client.

7. (Thrice amended) The system of claim [1] 6, wherein the security services examine a public key certificate to authenticate the client to determine the client privileges.

8. (Thrice amended) The system of claim [1] 6, wherein the security services use a digital signature to authenticate the client to determine the client privileges.

9. (Thrice amended) The system of claim [1] 6, wherein the host engine forwards to the client security code for enabling the client to perform a security protocol recognized by the security services.

10. (Thrice amended) The system of claim [1] 6, wherein one of the available services is secured by a firewall and one of the keys is configured to enable communication through the firewall.

11. (Twice amended) The system of claim [1] 6, further comprising a firewall for protecting the system.

12. (Thrice amended) The system of claim [1] 6, wherein one of the keys includes an address identifying the location of the selected service.

13. (Thrice amended) The system of claim [1] 6, wherein the code uses a key to provide to the client a direct connection with the selected service.

14. (Thrice amended) The system of claim [1] 6, further comprising a proxy for communicating with the selected service, and wherein the code enables the client to communicate with the proxy and one of the keys enables the proxy to locate the selected service.

Delete claim 15.

16. (Twice amended) The method of claim [15] 20, wherein establishing a communications link includes the step of using SSL to create a secure communications link with the client.

17. (Once Amended) The method of claim [15] 20, wherein establishing a communications link includes the step of negotiating an encryption protocol for transferring messages to and from the client.

18. (Once Amended) The method of claim [15] 20, wherein establishing a communications link includes the step of using public key certificates for transferring messages to and from the client.

19. (Twice amended) The method of claim [15] 20, wherein determining client privileges includes the step of using public key certificates to authenticate a user of the client.

20. (Twice amended) [The method of claim 15, wherein determining client privileges includes] A computer-based method comprising:

establishing a communications link with a client;

determining client privileges, the determining including the step of examining the identity of a user of the client and the level of authentication;

enabling the client to select a service from a set of available services, the set of available services based on the client privileges;

providing to the client service communication code that enables communication with a selected service; and

retrieving a key from a set of keys, each key corresponding to a respective service from the set of available services, the retrieved key for enabling communication between the client and the selected service, thereby enabling the client to access the available services without storing the service communication code and keys at the client.

21. (Twice amended) The method of claim [15] 20, wherein determining client privileges includes the step of examining a public key certificate to authenticate the client.

22. (Twice amended) The method of claim [15] 20, wherein determining client privileges includes the step of using a digital signature to authenticate the client.

23. (Twice amended) The method of claim [15] 20, wherein establishing a communications link includes forwarding to the client security code for enabling the client to perform a recognized security protocol.

24. (Thrice amended) The method of claim [15] 20, further comprising the step of using one of the keys to communicate through a firewall to the selected service.

25. (Twice amended) The method of claim [15] 20, wherein the method is performed by a server and further comprising using a firewall to protect the server.

26. (Thrice amended) The method of claim [15] 20, wherein one of the keys includes an address identifying the location of the selected service.

27. (Twice amended) The method of claim [15] 20, wherein providing includes the step of providing to the client a direct connection with the service.

28. (Thrice amended) The method of claim [15] 20, further comprising using a proxy to communicate with the service, and wherein providing includes enabling the client to communicate with the proxy.

29. (Four times amended) A system on a server computer system, comprising:

means for establishing a communications link with a client;

means for determining client privileges including means for examining the identity of a user of the client and the level of authentication;

means for enabling the client to select a service from a set of available services, the set of available services based on the client privileges;

means for providing to the client service communication code that enables communication with a selected service; and

means for retrieving a key from a set of keys, each key corresponding to a respective service from the set of available services, the retrieved key for enabling communication between the client and the selected service, thereby enabling the client to access the available services without storing the service communication code and keys at the client.

30. (Four times amended) A computer-based storage medium storing a program for causing a computer to perform the steps of:

establishing a communications link with a client;

determining client privileges <u>including examining the identity of a user of the client and the level of authentication;</u>

enabling the client to select a service from a set of available services, the set of available services based on the client privileges;

providing to the client service communication code that enables communication with a selected service; and

retrieving a key from a set of keys, each key corresponding to a respective service from the set of available services, the retrieved key for enabling communication between the client and the selected service, thereby enabling the client to access the available services without storing the service communication code and keys at the client.

Delete Claim 31.

32. (Once Amended) [A method according to claim 31, wherein the security information is received] <u>A method, comprising:</u>

<u>receiving, from</u> [the] <u>a client, as an advance communication, security information corresponding to one or more secured network services;</u>

<u>storing the security information at a location remote from the client;</u>

receiving a client request from the client to access a secured network service; and

using the stored security information to enable the client access to the secured network service without requiring the client to supply the stored security information.

33. (Once Amended) A method according to claim [31] 32, wherein the security information includes one or more keys corresponding to respective ones of the secured network services.

34. (Once Amended) A method according to claim [31] 32, wherein at least one of the keys includes a certificate for accessing at least one of the secured network services.

35. (Once Amended) A method according to claim [31] 32, further comprising determining client privileges of the client, and wherein the using the stored security information is provided if the privileges correspond to privilege requirements of the secured network service.

36. (Once Amended) A method according to claim [31] 32, further comprising determining client privileges of the client and enabling the client to select a service from ones of the secured network services corresponding to the determined client privileges.

37. (Once Amended) A system, comprising:

means for receiving, from a client, as an advance communication, security information corresponding to one or more secured network services;

means for storing the security information at a location remote from [a] the client;

means for receiving a client request from the client to access a secured network service; and

means for using the stored security information to enable the client access to the secured network service without requiring the client to supply the stored security information.

38. (Once Amended) A computer-readable storage medium storing program code for causing a computer to perform the steps of:

receiving, from a client, as an advance communication, security information corresponding to one or more secured network services;

storing the security information at a location remote from [a] the client;

receiving a client request from the client to access a secured network service; and

using the stored security information to enable the client access to the secured network service without requiring the client to supply the stored security information.